

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-183641

(43)Date of publication of application : 28.06.2002

(51)Int.Cl.

G06F 17/60

(21)Application number : 2000-385706

(71)Applicant : SUMITOMO CORP
CHUHAJO SOGO
KENKYUSHO:KK

(22)Date of filing : 19.12.2000

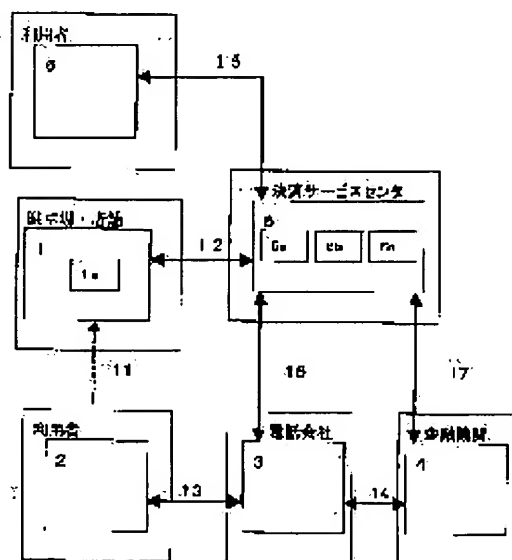
(72)Inventor : SHIGEMATSU ATSUSHI
OGITA TAKEYUKI
ISOBE TOSHIYA
MORI FUSAO
ISHIKAWA KOJI
OSHIMA TASUKU
KOJIMA MASAO

(54) PRINCIPAL CONFIRMING METHOD AND SYSTEM USING PORTABLE TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a principal confirming method and a principal confirming system required in cashless settlement of a service charge, such as the use of a parking garage, shopping and a mail-order sale in a store, and use of Internet ASP.

SOLUTION: This principal authenticating method required in the cashless settlement, comprises a procedure (a step 1) for informing a control device arranged in a providing site of commodity and service of a telephone number of a portable information terminal possessed by a user, a procedure (a step 2) for informing a settlement control device of the telephone number of the information terminal from a control device, a procedure (a step 3) for inquiring whether to approve to perform settlement by presenting a demand cause and the amount by telephoning to the information terminal of the telephone number from the settlement control device, and a procedure (a step 4) for confirming the principal, by confirming the input of the effect of approving the perform the settlement.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the

examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-183641

(P2002-183641A)

(43) 公開日 平成14年6月28日 (2002.6.28)

(51) Int.Cl.⁷

G 0 6 F 17/60

識別記号

4 1 4

Z E C

5 0 6

F I

G 0 6 F 17/60

テ-マコ-ト* (参考)

4 1 4

Z E C

5 0 6

5 B 0 4 9

審査請求 未請求 請求項の数10 O L (全 17 頁)

(21) 出願番号 特願2000-385706 (P2000-385706)

(22) 出願日 平成12年12月19日 (2000.12.19)

(71) 出願人 000002129

住友商事株式会社

東京都中央区晴海一丁目8番11号

(71) 出願人 598121606

株式会社駐車場総合研究所

東京都渋谷区宇田川町2番1号 渋谷ホームズ1205号

(72) 発明者 重松 篤

愛知県名古屋市昭和区丸屋町6-67

(74) 代理人 100085028

弁理士 西森 浩司

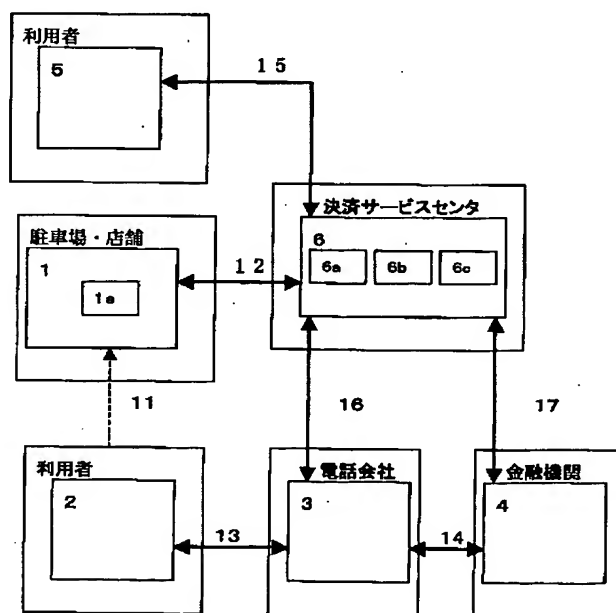
最終頁に続く

(54) 【発明の名称】 携帯端末を利用した本人確認方法及びシステム

(57) 【要約】

【課題】 駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人確認方法及び本人確認システムを提供する。

【解決手段】 非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ1)と、管理装置から決済管理装置に、情報端末の電話番号を通知する手順(ステップ2)と、決済管理装置から当該電話番号の情報端末に電話を掛け、請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順(ステップ3)と、決済を行うことを許諾する旨の入力を確認することにより本人確認を取る手順(ステップ4)とを含んで構成されている。



【特許請求の範囲】

【請求項1】 駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、前記管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、前記決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、そして、前記情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証を行う手順と、を含んで構成されてなる本人確認方法。

【請求項2】 請求項1に記載の本人確認方法において、本人確認を取る手順は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて使用する手順からなることを特徴とする本人確認方法。

【請求項3】 請求項1又は2に記載の本人確認方法において、利用者から前記管理装置への通知手順は、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力する手順からなることを特徴とする本人確認方法。

【請求項4】 請求項1又は2に記載の本人確認方法において、本人確認を取る手順は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする本人確認方法。

【請求項5】 請求項1又は2に記載の本人確認方法において、本人確認を取る手順は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする本人確認方法。

【請求項6】 駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人認証システムにおいて、電話機能を持った携帯可能な情報端末と、商品・サービスの提供サイトに設けられ、利用者から入力された少なくとも利用者の所持する携帯可能な情報端末の電話番号を決済管

理装置に通知する電話番号通知手段を有してなる管理装置と、携帯可能な情報端末及び管理装置に公衆電話回線等の通信回線を用いて接続され決済サービスセンタに設けられた決済管理装置であって、管理装置から通知された利用者の所持する携帯可能な情報端末の電話番号に基づいて当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段と、利用者の有する携帯可能な情報端末から決済を行うことを許諾する旨の入力を確認することにより非現金決済において必要となる本人確認手段とを有してなる決済管理装置と、を含み構成されてなる本人確認システム。

【請求項7】 請求項6に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等の携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて本人確認するようにしてなることを特徴とする本人確認システム。

【請求項8】 請求項6又は7に記載の本人確認システムにおいて、前記管理装置は、利用者が直接必用事項を入力することができる入力装置、利用者が所持している携帯可能な情報端末から無線通信により非接触入力することができる受信装置、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力された入力信号を変換する入力信号変換装置のいずれか又はそれらの任意の組み合わせを含んでなることを特徴とする本人確認システム。

【請求項9】 請求項6又は7に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号とを照合・確認するようにしてなることを特徴とする本人確認システム。

【請求項10】 請求項6又は7に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認するようにしてなることを特徴とする本人確認システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人確認方法及び本人確認システムに係り、特に、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証

を各種の非現金決済において必要となる本人であることの確認に利用した本人確認方法及び本人確認システムに関する。

【0002】

【従来の技術】駐車場や店舗や通信販売やインターネットのASPなどの利用料金を支払う場合、各種の方法が存在していた。

1) 現金での支払は、最も単純で金銭の授受という点では最も確実な方法である。また、通信販売においては、代金引換えや商品受け取り後に郵便為替等による支払も行われていた。

2) クレジットカードによる支払では、当該カードを商品・サービスの提供サイトに設けられたカードリーダー(読取機)に通し磁気ストリップに記録された暗証番号等を読み取り、一方、利用者に暗証番号を言わせて照合する。かかる照合により本人であることを確かめた後(本人確認後)、当該取引についての決済を行う。カードリーダーの無い場合には、カード裏面に設けられたサイン欄に記述のサインとの照合により確認を行う。

【0003】3) デビットカードでは、金融機関のキャッシュカードを使って、小売店での買い物時に利用者の預金口座から代金を引き落とし、小売店が指定した口座に入金する。クレジットが与信枠を設けるのに対し、デビットは即時決済を行う点で相違している。デビットカード利用者が本人であることの確認は、クレジットカードと同様で、カードリーダー(読取機)によるか、サインの照合によって行っている。消費者にとっては、現金を持たずに買い物できる上に即時決済できるという利便性がある。一方、小売店にとっては、クレジットカードよりも安い手数料で即時に売上金が回収できる利点がある。

4) プリペイドカードによる支払方法では、利用者がそのカードを購入した本人であるか否かは問わず、カードに記述された残高から利用した分だけ差し引き、利用可能な金額を更新する。小銭が不要で決済が短時間で済む、割引やプレミアム、カードデザインのファッション性等により普及が促進されている。最近では、バスネット等1枚のカードで複数の鉄道、バスを利用できるものが発行されて人気を集めている。

【0004】5) 一風変わった支払方法としては、ダイヤルQ2がある。ダイヤルQ2では、利用者が自己の電話機能を持った情報端末を使用し、この情報端末から情報が登録されているサービス提供会社に電話をかけ利用する。この場合の料金は、利用した情報量により課金される。すなわち、電話会社がサービス提供会社に代行して情報端末を所有する利用者から、具体的には、その電話番号の電話料金と一緒に利用料金の徴収を行っている。この場合、サービス提供会社により提供される情報を利用する者が当該情報端末の所有者であるか否かは、暗証番号の照合程度の簡単な確認により行っているに

過ぎなかった。

6) 営業などのビジネスにおいて、PCやPDAなどの携帯端末からデータサーバへアクセスした場合の使用料金は、利用者が誰であるかの認証を行った上で予め決めてあった支払方法に従って決済する。この場合の認証は、付属の装置を付けるなど改造が必要である。

【0005】

【発明が解決しようとする課題】前述した第一の支払方法は、現金をいつも持ち歩かなければならない関係から落としたり盗難にあう危険がつきまとう。また、駐車場の場合のように小銭が無い場合には利用できな。また、雨の日には濡れて紙幣が使えなくなるなどの欠点があった。さらに、代金引換えや郵便為替による支払は、その時に現金の持ち合わせがないと商品を受け取れない。また、郵便局に行って所定の手続きをしなければならない煩わしさが有る。

【0006】かかる事情により現金を用いない支払方法の開発が要望されていた。かかる要望に応えたものが前記2)~4)であるが、クレジットカード及びデビットカードによる支払は、盗難や拾い物によって入手した第三者が不正使用した場合に大きな被害をもたらす恐れがある。従って、そのカードを使用しようとする者が、カード所有者本人であることを確かめること、すなわち、本人確認を取ることが重要な事項となる。

【0007】従来、本人であることの確認は、カード裏面の磁気ストリップに記録された暗証番号と利用者が言った暗証番号との照合、又は、カード裏面に設けられたサイン欄に記述のものと利用者が利用明細書に記載したサインとの照合により行っていた。前者の方法では、磁気ストリップに記録された事項を読み取ることができる機器の登場により不正使用に太刀打ちすることができなくなった。かかる欠点を無くし且つカードに蓄積できる情報量を増大したものとしてICチップを埋め込んだクレジットカードも誕生している。しかしながら、価格の点で実用化に至っていない。後者の方では、海外で使用された場合を除いて、サインを真似て練習されると本物と見分けがつかないというのが実情であった。

【0008】プリペイドカードは、利用者が事業者に与信を与える関係となり、代金後払いのクレジットカードの場合と逆である。プリペイドカードに割引やプレミアムが設定される所以である。その関係から、高額のもの購入には不向きで汎用性に欠ける欠点があった。利用時に本人確認が行われない関係から、盗難や落し物をした場合には回収不可能となっていた。なお、プリペイドカードは、販売した時点で事業者が所期の利益を得てしまうため、利用者保護のための認証システムの構築には不熱心である事情がある。

【0009】ダイヤルQ2は、公衆回線等の通信回線を用いて利用者がサービス提供会社に電話をかけ情報を利用した場合に、情報量に応じた利用料金を電話会社がサ

ービス提供会社に代わって徴収する。電話会社は、当該情報の利用に関連して公衆回線を利用したことに対する利用料金を、当該情報端末の契約者を発信者情報を入力することにより特定して徴収する。これにより、利用料金徴収の効率化が図れる。しかしながら、ダイヤルQ2は、クレジットカードの場合と同様に、暗証番号の照合程度の簡単な確認により利用可能である。従って、暗証番号が漏れた場合等における不正使用に対しては実質的に対処不能である欠点があった。PCやPDAなどの携帯端末からデータサーバへアクセスした場合の使用料金は、利用者が誰であるかの認証を行った上で予め定めてあった支払方法に従って決済する。この場合の認証は、付属の装置を付けることによって確実に行われるが、付属装置の価格が比較的高価である欠点があった。

【0010】よって、本発明は、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証を各種の非現金決済において必要となる本人であることの確認に利用した本人確認方法及び本人確認システムを提供することを目的とする。本発明は、また、本人確認の精度を向上させることができる本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらに、適宜の手法で携帯可能な情報端末の電話番号を管理装置に通知することができる本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらにまた、簡単な構成により本人確認の精度を向上させることができる他の本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらにまた、簡単な構成により本人が商品・サービスの提供サイトなど、その場所から入力することを特定する本人確認方法及び本人確認システムを提供することを目的とする。

【0011】

【発明が解決しようとする手段】本発明は、上述した目的を達成したもので、駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に利用者から少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、そして、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証を行う手順とを含んで構成されてなる本人確認方法を提供する。

【0012】請求項2に記載の発明は、請求項1に記載の本人確認方法において、本人確認を取る手順は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて使用する手順からなることを特徴とする。請求項3に記載の発明は、請求項1又は2に記載の本人確認方法において、利用者から管理装置への通知手順が、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力する手順からなることを特徴とする。

10

20

【0013】請求項4に記載の発明は、請求項1又は2に記載の本人確認方法において、本人確認を取る手順が、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする。請求項5に記載の発明は、請求項1又は2に記載の本人確認方法において、本人確認を取る手順が、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする。

30

40

【0014】本発明の第二の態様は、駐車場利用や店舗での買物や通信販売、インターネットASP利用などの利用料金の非現金決済において必要となる本人であることの確認を取る本人確認システムにおいて、電話機能を持った携帯可能な情報端末と、商品・サービスの提供サイトに設けられ、利用者から入力された少なくとも利用者の所持する携帯可能な情報端末の電話番号を決済管理装置に通知する電話番号通知手段を有してなる管理装置と、携帯可能な情報端末及び管理装置に公衆電話回線等の通信回線を用いて接続され決済サービスセンタに設けられた決済管理装置であって、管理装置から通知された利用者の所持する携帯可能な情報端末の電話番号に基づいて当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段と、利用者の有する携帯可能な情報端末から決済を行うことを許諾する旨の入力を確認することにより非現金決済において必要となる本人であることの確認を取る本人確認手段とを有してなる決済管理装置とを含み構成されてなる本人確認システムを提供する。

50

【0015】請求項7に記載の発明は、請求項6に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、携帯可能な情報端末の電話登録暗証番号、氏

名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせる本人確認するようにしてなることを特徴とする。

【0016】請求項8に記載の発明は、請求項6又は7に記載の本人確認システムにおいて、管理装置は、利用者が直接必用事項を入力することができる入力装置、利用者が所持している携帯可能な情報端末から無線通信により非接触入力することができる受信装置、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力された入力信号を変換する入力信号変換装置のいずれか又はそれらの任意の組み合わせを含んでなることを特徴とする。請求項9に記載の発明は、請求項6又は7に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号とを照合・確認するようにしてなることを特徴とする。

【0017】請求項10に記載の発明は、請求項6又は7に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認するようにしてなることを特徴とする。

【0018】

【発明の実施の形態】以下、図面を用いて本発明の本人確認方法及び本人確認システムを詳細に説明する。図19は、本発明に係る本人確認システムの一実施形態のブロック図である。図19に示すように、本人確認システムの一実施形態は、概略的に、携帯電話等の電話機能を持った携帯可能な情報端末2と、商品・サービスの提供サイトに設けられた管理装置1と、そして、管理装置1及び情報端末2に公衆電話回線等の通信回線を介して接続された決済管理装置6とを備えて構成されている。利用者は、管理装置1にある入力装置、例えば、テンキーや画面の数字部位を押圧することにより少なくとも利用者の所持する情報端末2の電話番号を入力することができる。管理装置1は、当該電話番号をメモリに記録すると共に決済管理装置6に通知する。これらの操作は、管理装置1に設けられた電話番号通知手段1aによって行われる。

【0019】決済管理装置6は、本システムを維持/管理する決済サービスセンタに設けられるもので、管理装置1から通知された利用者の所持する携帯可能な情報端末2の電話番号に基づいて当該電話番号の情報端末に電話を掛ける制御手段6aを備えている。決済管理装置6は、また、情報端末2の表示画面に少なくとも請求原

因、例えば、XX駐車場における駐車料金であるとか〇〇デパートにおける買い物であるとかの表示とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段6bと、そして、利用者の有する携帯可能な情報端末2から決済を行うことを許諾する旨の入力を確認する本人確認手段6cとを有している。

【0020】図示された好ましい実施例では、情報端末2は、電話会社の電話管理装置3を介して公衆回線13、16で決済管理装置6と接続されている。使用された電話料金及び商品・サービスの提供サイトにおける利用料金は、本人確認後に、金融機関等の決済装置4により決済される。従って、決済管理装置6と決済装置4とは、一般の又は専用の通信回線17によって接続されている。使用された電話料金及び商品・サービスの提供サイトにおける利用料金は、また、決済管理装置6の代わりに、ダイヤルQ2と同様に、電話会社により代行徴収するように構成することもできる。この場合、電話管理装置3と決済装置4とは、一般の又は専用の通信回線14によって接続される。

【0021】図20は、図19に示された本人確認システムによって実行される本発明に係る本人確認方法の一実施形態のフローチャートである。図示されているように、本発明に係る本人確認方法は、商品・サービスの提供サイトに設けられた管理装置に利用者から少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ1)と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ2)と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順(ステップ3)と、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人であることの確認を取る手順(ステップ4)とを含んで構成されている。

【0022】本発明方法では、日本人であればほとんどの人が所持している携帯可能な情報端末の電話番号を商品・サービスの提供サイトに設けられた管理装置1において利用者から取得し、これを決済管理装置6に通知し、さらに決済管理装置6から当該通知された情報端末2の電話番号を用いて電話を掛け、その情報端末2をその時携帯している者から何らかの行動、具体的には、決済を行うことを許諾する旨の入力か、又は、全く心当たりがないことを理由とする拒否する旨の入力を確認する。管理装置1に情報端末2の電話番号を入力している者がその情報端末2をその時携帯している者でない場合には、全く心当たりがないことを理由とする拒否することとなる。逆に、決済を行うことを許諾する旨の入力があつた場合には、管理装置1に情報端末2の電話番号を入力している者がその情報端末2をその時携帯している

者であることを、実質的に証明することとなる。これにより、本人であることの確認が取れることになり、決済の手続きに移行させることができる。

【0023】なお、携帯電話の盗難や落し物等により、契約者以外の者の手に携帯可能な情報端末2が渡る可能性も否定できない。このような場合、クレジットカードやデビットカードと同様に、不正拾得者の使用を当該携帯可能な情報端末2の契約者の使用ではないと見破ることはできない。そこで、図示された好ましい実施例では、携帯可能な情報端末そのものには記録されていない各種の個人情報、例えば、携帯可能な情報端末2の電話登録暗証番号、契約者の氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号、指紋など生体データ等、携帯可能な情報端末2の契約者のみが知り得る個人情報のいずれか1つ又は複数を、携帯可能な情報端末2（又は管理装置1）から入力させ、電話会社又は決済管理装置6のメモリに記録されている対応するデータと照合することにより（ステップ5）、本人であることの認証精度を向上させることができる。

【0024】

【具体例1】図1は、駐車場における本人確認システム及びそれを利用した利用料金決済システムのブロック図である。この利用料金決済システムは、従来、現金や各種のカード、例えば、クレジットカード、デビットカード、プリペイドカード等を用いて支払っていた利用料金を、電話会社が携帯電話の口座から代行徴収するようにしたものである。図示された本人確認システムは、概略的に、駐車場に隣接して設置された管理装置1と、管理装置1に有線、無線各種の通信回線12を介して接続された決済管理装置6と、駐車場を利用する者が所持する携帯電話等の携帯可能な情報端末2と、情報端末2と決済管理装置6とを通信回線13、16を介して接続する電話管理装置3と、そして、電話管理装置3及び決済管理装置6に通信回線14、17を介して接続された決済装置4とを含んで構成されている。尚、通信回線13の少なくとも一部は、情報端末2が携帯可能な情報端末であるため無線通信となる。

【0025】本システムは、自宅のPCを用いた場合等のインターネットを介しての通信販売やASP利用の利用料金の支払に伴う認証にも利用することができる。この場合、利用者が用いる情報端末5は、公衆電話回線等の通信回線15を用いて決済管理装置6に接続され、さらに、インターネット上のバーチャルショップ等には、通信回線12を介して接続される。また、認証に用いる情報端末2の電話番号も、決済管理装置6を経由して管理装置1に通知される。その後は、駐車場等における管理装置1と同様の手順によって、当該バーチャルショップ等を利用した者が、情報端末2の電話会社と契約した

本人であることを認証する。情報端末5は、また、決済管理装置6を経由せずにインターネットを介して直接アクセスするように構成することもできる。

【0026】駐車場の利用者が所定の情報を管理装置1に入力する際に、管理装置1に設けられたテンキーや画面に表示された数字/文字の部位を押圧することによって行うこともできる。その代わりとして、赤外線等の無線通信により非接触で行うこともできる。車の中から利用者が身を乗り出して入力をする必要がなく、また、雨の日など濡れなくてすむ利点がある。

【0027】管理装置1は、複数の駐車場に設置される入出場による利用料金を精算する管理装置である。駐車場は、自走ゲート式、コイン式、立体機械式、路上駐車式などである。また、駐車場以外の施設であって入場出場により料金を支払う施設、例えば、レンタカー貸し出し施設などにも設置可能である。また、複数の店舗における買物においても応用可能で、料金を精算するPOSレジに組み込んで設置可能である。店舗は、店員により商品を販売する商店だけでなく、自動販売機など無人の販売機械を含む概念である。前述のように、実販売のほかインターネットなどによる通信販売、インターネットのASP利用によるバーチャルショップも含まれる。

【0028】図2は、図1に示された管理装置1の詳細構成図であり、図3は、駐車場における管理装置1のデータ入力部104の一例を示す詳細構成図である。図4は、情報端末2の詳細構成図であり、図5は、電話管理装置3の詳細構成図である。図6は、決済管理装置6の詳細構成図であり、図7は、小売店等の店舗に管理装置1が設置される場合におけるデータ入力部104の詳細構成図であり、そして、図8は、情報端末5の詳細構成図である。

【0029】図2に示されている管理装置1の料金計算・課金部101は、入場時間と出場時間から利用料金の計算と売上処理とをし、利用者に対して課金処理をする。後述する店舗使用・通信販売では、買物の集計と売上処理とをし、課金処理をする。表示部102は、各種のデータを表示する液晶画面等の画像表示部である。この部位に、数字/文字キーを表示させ、これをテンキーの代わりとして使用することもできる。電話部103及び109は、電話の送受信、電話番号の通知、暗証番号の記録、電話機器番号など電話機能による照合、認証などを行う。テンキーや表示部102に表示された数字/文字エリア等を含むデータ入力部104は、利用者が所持している携帯可能な情報端末2の電話番号、認証の精度を向上させるための情報端末2の契約者のみが知り得る個人情報を入力する。

【0030】認証部105は、データ入力部104からの各種データと記録部106に記録された認証データ、課金データ、決済データ等のデータとを照合し認証する。決済データ部111は、予め利用者の住所、氏名、

年令、郵便番号、電話番号、決済口座番号（銀行カード、クレジットカード、デビットカード）など認証の精度向上を図ると共に決済に必要なデータを記録する。時計部 110 は、年月日時を発生するクォーツ時計等の時計からなる。制御部 107 は、上記各構成要素を用いて本発明に係る本人確認方法を実行するプログラムを制御する。なお、参照番号 108 は、管理装置 1 を小売店等の店舗に配置した場合における、取扱商品の詳細情報を蓄積する商品データ部である。

【0031】図 3 に示されているデータ入力部 104 は、ゲート式駐車場に用いられる管理装置 1 におけるもので、入場しようとする車を検知する入場検知部 1001 と、出場しようとする車を検知する出場検知部 1002 と、入場する車の特定のための入力を行う入場テンキー部 1003 と、そして、出場しようとする車の特定のための入力を行う出場テンキー部 1004 とを備えて構成されている。なお、出場テンキー部 1004 は、出場検知部 1002 からの検出信号と入場検知部 1001 からの検出信号とにより入出を識別できるため、省略することができその場合は入場テンキー部 1003 で代用する。

【0032】図 7 に示されているデータ入力部 104 は、店舗に設置される管理装置 1 におけるもので、買物の料金や認証データの基礎となるデータを入力する POS レジのカードリーダ部 2001 とテンキー部 2002 とを含んでいる。買物の料金を各種カードで支払う場合に、カード会社の認証方法に加えて本発明の認証により本人であることの確認を得る。例えば、本人であることに多少の疑義がある場合に、本人が所持しているであろう携帯電話に決済管理装置 6 から電話を掛け、その場で決済管理装置 6 からの電話を受ける動作により本人確認を行う。利用者は、決済管理装置 6 からの利用料金の課金対象として、カードとすることも電話料金の支払口座とすることもできる。

【0033】この場合、カード裏面に設けられた磁気ストリップ、IC カードのメモリなどに情報端末 2 の電話番号を記録しておくように構成することもできる。買物時に、カードリーダにカードを通してスワイプ操作すると、手動入力より迅速且つ間違いなく情報端末 2 の電話番号を入手することができる。そして、これを決済管理装置 6 に通知することができる。また、カード内に予め認証データを入れておくことで、決済管理装置 6 は電話会社に認証データを照会しなくても情報端末 2 からの認証データと照合・認証することもできる。また、上記テンキーの代わりに赤外線送受信機等の非接触入力装置を用いることもできる。

【0034】図 4 に図示された情報端末 2 は、利用者が携帯する携帯電話、PDA などの情報電話端末であって、決済諾否入力部 201 と、表示部 202 と、電話の受発信機能を有する電話部 203 と、データ入力部 20

4 と、認証部 205 と、記録部 206 と、そして、制御部 207 とを含んで構成される。各部における基本的機能は、前述した管理装置 1 における対応する構成要素のそれと同様であるので、詳細な説明は省略する。また、情報端末 2 と管理装置 1 とに、それぞれ赤外線受発信素子を別途に設けることで、非接触で情報端末 2 のデータ入力部 204 から入力した各種のデータを管理装置 1 へ入力することができる。また、指紋入力部を別途設けることで認証することができる。

【0035】図 8 に図示された情報端末 5 は、通信販売利用時やインターネットの ASP 利用時に、利用者が用いるものである。駐車場や小売店等の店舗における本人確認方法では、利用者が商品・サービスの提供サイトに設けられた管理装置 1 の場所で認証データの入力を行う。それに対して、本実施例のような通信販売利用やインターネットの ASP 利用では、利用者は遠隔地からインターネット等の通信回線を介して管理装置 1 に接続される。利用者端末 5 は、携帯可能な、または、卓上の携帯電話、PDA、パソコンなどの情報通信端末であって、決済諾否入力部 501 と、表示部 502 と、電話の受発信機能を有する電話部 503 と、データ入力部 504 と、認証部 505 と、記録部 506 と、そして、制御部 507 とを含んで構成される。各部における基本的機能は、前述した管理装置 1 における対応する構成要素のそれと同様であるので、詳細な説明は省略する。

【0036】図 5 に図示された電話管理装置 3 は、NTT ドコモ社等の携帯電話会社に設置されるもので、電話番号によって特定される外部の情報端末 2 に回線を接続する電話部 301、302、307 と、認証データや決済データを予め登録しておく決済データ部 304 と、情報端末 2 の機器識別データやサービス・物販識別データなどの認証を行う認証部 305 と、そして、駐車場や店舗などでの利用料金や通話料金は受信先課金機能などにより課金するが、これらデータを記録する記録部 306 とを備えて構成されている。

【0037】図 6 に示された決済管理装置 6 は、決済サービスセンタに設けられるもので、電話番号によって特定される外部の端末、例えば、電話管理装置 3 や決済装置 4 に回線を接続する電話部 601、602、607 と、電話料金、課金データの内の利用料金及び決済データを決済装置 4 に送信し決済する等の制御を行う制御部 603 と、認証データや決済データを予め登録しておく決済データ部 604 と、電話管理装置 3 からの認証データ、課金データ及び決済データと管理装置 1 からの認証データ、課金データ及び決済データとを照合し認証する認証部 605 と、電話料金、課金データの内の利用料金及び決済データを記録する記録部 606 とを含んで構成されている。図示された好ましい実施例では、さらに、地図情報を記録した地図データ部 608 も有している。無人管理の場合に、管理装置 1 の場所と関連づけするこ

とにより、複数の管理装置1の利用状況を固定または携帯可能な情報端末（図示せず）で把握管理することができる。

【0038】金融機関の決済装置4は、電話管理装置3からの電話料金と課金データの内の利用料金などを、利用者口座から電話会社口座へ、また、電話会社口座から駐車場、店舗口座へ振替え決済をする。通信回線12、13、14、15、16、17は、必用に応じて、ISDN回線、インターネット回線、PHS回線などの種々の回線手段を用いることができる。認証データは、予め電話会社の電話管理装置3と、決済サービスセンタの決済管理装置6と、駐車場・店舗の管理装置1（店舗のPOSレジ）に使用されるカード内の1つ以上に記録することができる。

【0039】この認証データとしては、情報端末2の電話番号の他、（1）自由な暗証番号、管理装置1が自動的に発行するランダムな暗証番号、電話利用以外のソフト情報・物販などで利用する利用者識別番号であるサービス・物販利用者識別データ、発信者番号通知による電話番号、電話機器識別データである電話機器番号、管理装置1の電話番号、管理装置1の装置識別データである装置番号、情報端末2から入力する諾否データや管理装置1の自動発行にかかる決済番号である決済の諾否データ、及び、（2）情報端末2の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号と、決済データの暗証番号、指紋など生体データなど情報端末2の契約者のみが知っている個人情報である。前者は、携帯端末である情報端末2とシステムの各装置との間の相互の認証に、後者は利用者本人であることの確認の精度向上のためのデータとして使用する。

【0040】課金データは、年月日時、データ管理番号、駐車場名、入出場時間、店舗名、通販管理番号、商品名、数量、利用料金（金額）などからなる。受信者課金データは、受信者に課金するデータの識別番号である。サービス・物販識別データは、電話利用以外のソフト情報・物販などの識別番号である。決済データは、予め利用者が登録する銀行の決済口座番号、クレジットカード番号などで、氏名、年令、住所、郵便番号、電話番号、暗証番号など個人を特定するデータとリンクし、決済を可能とするデータである。入場の有無データは、駐車場の利用の有無を管理装置1のデータ入力部104より入力する有り：1、無し：0と自動発行される決済番号である。

【0041】次に、図9～図11を用いて、ゲート式駐車場を利用する場合における本発明に係る本人確認方法及び認証後における決済の流れを説明する。図9は、ゲート式駐車場に車を入場する時の流れを示すフローチャートである。図10は、ゲート式駐車場から車を出場す

る時の流れを示すフローチャートである。図11は、ゲート式及びコイン式駐車場を利用した場合のデータ表の一例である。図9に示されているように、ゲート式駐車場に入場しようとする、管理装置1の入場検知部1001（図3参照）が車の進入を検知する（ステップ11）。この時、利用者は、入場テンキー部1003から利用者の認証データのうち、少なくとも情報端末2の電話番号と自由な暗証番号を入力する（ステップ12）。高いセキュリティを求めるときは、情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末2の契約者のみが知り得る個人情報も同時に入力する。

【0042】管理装置1の認証部105に、上記電話番号を照会し、入場がないことをチェックした後、管理装置1の記録部106に認証データのうち少なくとも情報端末2の電話番号と自由な暗証番号と入場時刻を記録する（ステップ13）。次に、電話部103から決済管理装置6の第1電話部601（図6参照）に電話し、データに入場有りデータを追加し、送信する（ステップ14）。決済管理装置6は、データにサービス・物販識別データ（例えば、駐車場料金を示す#0880などの文字列）と、受信者課金データ（例えば、XXX氏への課金を行うためのデータである#108などの文字列）とを追加し、記録部606に記録する。一方、第2電話部602から電話管理装置3の第1電話部301に電話し、前記データを送信する（ステップ15）。

【0043】電話管理装置3では、決済データ部304に記録された認証・決済データと、前記データのサービス・物販識別データと、そして、受信者課金データとを認証部305で認識し、記録部306に記録する。並行して、情報端末2に前記データの内、サービス・物販識別データ以外のデータを送信する（ステップ16）。利用者は、情報端末2から認証データのうち少なくとも自由な暗証番号と入場の有データ“入場する：1”を入力し、管理装置1に返信する（ステップ17）。管理装置1の認証部105が認証データのうち少なくとも自由な暗証番号と入場の有データである“入場する：1”を認識した場合、それを記録部106に記録する。これにより、入場検知部1001のゲートが開き入場できる状態となる（ステップ18）。

【0044】また、入場の無データである“入場しない：0”の返信の場合は、入場できない状態が継続する。入場データは、また、決済サービスセンタの決済管理装置6に送信し、記録部606に記録する。決済管理装置6は、これら入場データから地図情報記録の手段及び管理装置1の場所と関連づけする手段を持つ地図データ部608で、複数の管理装置1の利用状況を把握することができる。また、第3電話部607から、このよう

な利用状況データを固定または携帯可能な情報端末に送信することができる。(図示なし)

【0045】一方、ゲート式駐車場から出場するときには、図10に示されているように、出場検知部1002で車を検知する(ステップ21)。この時、利用者は、出場テンキー部1004から、利用者の認証データのうち少なくとも情報端末2の電話番号と自由な暗証番号を入力する(ステップ22)。高いセキュリティを求めるときは、入場時に入力した個人情報、例えば、情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報も同時に入力する。駐車場の入場と出場において、管理装置1での照合・認証は、図11に図示したように、電話番号、駐車場名、入場ゲート関連番号と出場ゲート関連番号によって照合し、認証することによって短時間に照合・認証作業を完了することができる。

【0046】このように、管理装置1の認証部105で、認証データのうち少なくとも情報端末2の電話番号を照合、認証する(ステップ23)。記録部106には、電話番号及び自由な暗証番号と出場時刻を記録する。一方、入場時刻と出場時刻から利用料金を料金計算・課金部101で計算し、認証データのうち少なくとも情報端末2の電話番号及び自由な暗証番号から課金すべき口座を特定して課金し、並行して、課金データとして記録部106に記録する(ステップ24)。

【0047】管理装置1は、上記認証データである情報端末2の電話番号と自由な暗証番号とに課金データを追加し、決済サービスセンターの決済管理装置6に、これらを送信する(ステップ25)。決済管理装置6は、上記認証データである情報端末2の電話番号と、課金データに、(さらに、サービス・物販識別データ(例えば#0880などの文字列)と、受信者課金データ(例えば#108などの文字列)と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内等を追加しても良い。)自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置3を経由し情報端末2に送信する(ステップ26)。並行して、これらのデータは、

決済管理装置6の記録部606に記録される。

【0048】前記()内の追加データの場合、電話管理装置3の認証部305で、サービス・物販識別データと受信者課金データを認証し、課金すべき受信者毎に課金データ及び決済の諾否データを記録部306に記録し、並行して情報端末2に送信する(ステップ27)。利用者は、認証データである情報端末2の電話番号と課金データを確認する。(さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証

番号などを追加しても良い。)自由な暗証番号と、決済諾否データである“決済する：1”を入力し、電話管理装置3を経由し、決済管理装置6に送信する(ステップ28)。決済管理装置6は、上記認証データを照合・認証し、記録する。合格すると、認証データである、情報端末2の電話番号と、課金データと、(さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。)決済許諾データである“決済する：1”を、それぞれ、電話管理装置3と管理装置1に送信し、記録する。

【0049】管理装置1の出場検知部1001はゲートを開き、車両が出場できる状態とする(ステップ29)。また、決済の拒否データである“決済しない：0”の返信の場合は、出場できない。決済に際して決済管理装置6は、図12に示すように、認証データである情報端末2の電話番号と、課金データと、(さらに、電話機器識別データと、発信者番号通知の電話番号と、サービス・物販識別データ(例えば#0880などの文字列)と、受信者課金データ(例えば#108などの文字列)と、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。)を電話管理装置3に送信する(ステップ31)。

【0050】電話管理装置3は、認証部305に予め登録されている認証データと照合・認証する(ステップ32)。合格すると、認証データを決済管理装置6と、管理装置1と、そして、情報端末2に送信する。

(1) 電話管理装置3の料金の回収を決済管理装置6が代行する本実施例では、電話管理装置3から決済管理装置6を経由し、決済装置4へ利用者の決済口座番号と、課金データを送信し(ステップ37)、決済装置4で利用者の口座振替を行うことも可能である。決済装置4は、個々の携帯可能な情報端末利用者の口座から決済管理装置6の口座へ商品・サービス利用料金の振替を行う(ステップ38)。さらに、決済管理装置6の口座から商品・サービスの提供者である駐車場・店舗の銀行口座へ振替決済する(ステップ39)。この場合、電話料金は、電話管理装置3から決済装置4へ直接送信し、商品・サービスの利用料金とは別扱いになる。

【0051】また、料金の回収を決済管理装置6が行う場合に、予め認証データを決済管理装置6に登録して、これを用いて認証し、利用者の決済口座番号及び課金データを決済装置4へ送信し決済することも可能である。

(2) 一方、料金の回収を電話管理装置3が行う実施例では、電話管理装置3から金融機関の決済装置4へ情報端末2の電話番号の決済口座番号と、電話料金と、課金データを送信する(ステップ33)。決済装置4は、利用者の口座から電話会社の口座へ商品・サービス利用料金及び電話料金の振替を行う(ステップ34)。さらに、電話会社口座から、駐車場・店舗の銀行口座へ振替決済す

る(ステップ35)。

【0052】また、この場合に、氏名、郵便番号、年令、住所の一部、電子メールアドレス、支払先金融機関名、口座番号などを情報端末2から入力させ、認証することで一層の機器認証と本人確認のセキュリティを高めることができる。また、決済サービスセンターの決済管理装置6は、これら出場データから、地図情報記録手段及び管理装置1の場所と関連づけする手段を持つ地図データ部608で、複数の管理装置1の利用状況を把握することができる。また、第3電話部607から固定または携帯可能な情報端末に利用状況データを送信することができる。

【0053】また、管理装置1が自動的に発行するランダムな暗証番号を情報端末2に表示し、利用者が管理装置1から入力するランダムな暗証番号を管理装置1で照合・認証することも可能である。以上、ゲート式駐車場について詳細に説明したが、駐車時及び駐車終了時にそれぞれ図9及び図10に示された入場時及び出場時における操作を行うことにより、路上駐車式の駐車スペースに対しても応用可能である。また、この路上駐車場などで、入場時に最低利用料金を先に課金し、徴収することも可能で、さらに、追加利用料金を携帯電話から継続利用料金を行う課金データを送信することで継続使用が可能となる。また、ここに示した駐車場利用、店舗での買物、通信販売、インターネットのASP利用以外にもレンタル利用、ガソリンスタンド利用にも利用できる。

【0054】

【実施例2】次に、車両が駐車スペースに駐車した場合に、車両下方に設けられたフラップが所定高さまで持ち上がり車両の出場を許さないように構成したフラップ式駐車場利用の例について説明する。図13は、フラップ式駐車場に入場するときの流れを示すフローチャートであり、図14は、フラップ式駐車場から出場するときの流れを示すフローチャートである。フラップ式駐車場においては、入場時、入場検知部1001が車を検知する(ステップ41)と自動的に駐車スペースの番号に対応するフラップ番号と入場時刻が管理装置1の記録部106に記録される(ステップ42)。車両が当該駐車スペースに駐車してから所定時間後、入場検知部1001はフラップを所定高さまで持ち上げ車両が駐車スペースから出られないようにする(ステップ43)。なお、このため、ゲート式駐車場の入場時のように認証行為は行なわない(図9参照)。次に、出場部1002は、車両の駐車を検知し続けている(ステップ51)。出場に際して、駐車場利用者は、出場テンキー部1004からフラップの番号と、利用者の認証データのうち少なくとも情報端末2の電話番号と、そして、自由な暗証番号を入力する。管理装置1の記録部106にフラップ番号と上記電話番号と自由な暗証番号と出場時刻を記録する(ステップ52)。管理装置1の記憶部106に、フラップ番号と、

利用者が所有している情報端末2の電話番号と、自由な暗証番号、そして、出場時刻を記憶する(ステップ53)。

【0055】管理装置1の料金計算・課金部101は、入場時刻と出場時刻から利用料金を計算し、課金処理を行う(ステップ54)。次に、電話部103から決済管理装置6に電話をし、認証データと、そして、課金データとを送信する(ステップ55)。決済管理装置6は、認証データである情報端末2の電話番号と、課金データに、(さらに、サービス・物販識別データ(例えば#0880などの文字列)と、受信者課金データ(例えば#108などの文字列)と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内などを追加しても良い。)自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置3に送信する(ステップ56)。

【0056】電話管理装置3は、サービス・物販識別データと受信者課金データとを認証し、課金データと決済の諾否問合せデータを情報端末2に送信する(ステップ57)。前記()内の追加データの場合も、電話管理装置3で、サービス・物販識別データと受信者課金データを認証し、課金データと決済の諾否データを情報端末2に送信する。利用者は、情報端末2から認証データである情報端末2の電話番号と課金データ(さらに、サービス・物販識別データと、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。)を確認する。自由な暗証番号と、決済諾否データである“決済する：1”を入力し、電話管理装置3を経由し決済管理装置6に送信する(ステップ58)。

【0057】決済管理装置6は、上記認証データを照合・認証し、記録する(ステップ59)。合格すると、認証データである情報端末2の電話番号と、課金データと、(さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。)、決済許諾データである“決済する：1”を、電話管理装置3と管理装置1に送信する(ステップ60)。出場検知部1001のフラップが下がり(ステップ61)、車両は出場できる。また、決済の拒否データである“決済しない：0”の返信の場合は、出場できない。また、決済の方法や高いセキュリティの設定は、ゲート式駐車場利用の例と同様に行うことができる。また、機械式立体駐車場も同様な処理となる。

【0058】

【実施例3】次に、小売店等の店舗において買い物をする際に、その利用者が所持する携帯可能な情報端末2の電話会社による高信用力の認証を利用することにより、利用料金の課金及び決済する方法とシステムの例について説明する。図15は、店舗で買い物利用したときの流

れを示すフローチャートであり、図16は、店舗での買い物利用のデータ表例を示す図である。システムの詳細は、基本的に図1に示されたものと同様であるためその説明は省略する。

【0059】店舗で買い物利用したときの流れは、まず、店舗の管理装置1の料金計算・課金部101で買物料金の集計をし、課金処理をする。並行して、これを記録部106に記録する(ステップ71)。次に、図7に示されたデータ入力部104のカードリーダー部2001やテンキー部2002を用いて、利用者の認証データのう

ち少なくとも情報端末2の電話番号と自由な暗証番号を入力をする(ステップ72)。なお、カードに利用者の電話番号を記録しておき、買物時、カードリーダー部2001により当該記録を読み込むと手動入力より処理が早く且つ間違いないようにすることができる。

【0060】また、高いセキュリティを求めるときは、情報端末2の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報も同時に入力する。一方、管理装置1の記録部106は、データ管理番号(POS機器番号と売上連番)と、上記電話番号と、自由な暗証番号と、売上時刻を記録する(ステップ73)。管理装置1は、上記認証データである情報端末2の電話番号と自由な暗証番号に、課金データを追加し、決済サービスセンタの決済管理装置6にこれらを送信する(ステップ74)。

【0061】決済管理装置6は、上記認証データである情報端末2の電話番号と課金データに(さらに、サービス・物販識別データ(例えば#0880などの文字列)と、受信者課金データ(例えば#108などの文字列)と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内などを追加しても良い。)、自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置3を経由し情報端末2に送信する(ステップ75)。

【0062】前記()内の追加データの場合も、電話管理装置3で、サービス・物販識別データと受信者課金データを認証し、課金データと決済の諾否データを情報端末2に送信する。利用者は、携帯可能な情報端末2で、認証データである情報端末2の電話番号と、課金データを確認する。(さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。)しかる後、自由な暗証番号と、決済諾否データである“決済する:1”を入力し、電話管理装置3を経由し決済管理装置6に送信する(ステップ76)。

【0063】決済管理装置6は、上記認証データを照合・認証し、記録する(ステップ77)。合格すると、認証データである情報端末2の電話番号と、課金データと、

(さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。)決済許諾データである“決済する:1”を電話管理装置3と管理装置1に送信する(ステップ78)。

情報端末2から認証データのうち少なくとも自由な暗証番号と決済の許諾データである“決済する:1”が管理装置1に返信されると、管理装置1の認証部105で認証データのうち少なくとも自由な暗証番号と決済の許諾データである“決済する:1”を認証し、記録部106に記録し、売上処理を終了する(ステップ79)。決済管理装置6は、さらに、電話管理装置3に課金データを送信する(ステップ80)。また、決済の拒否データである“決済しない:0”の返信の場合は、売上処理することなくキャンセルする。また、決済の方法や高いセキュリティの設定は、前述したゲート式駐車場利用の例による。

【0064】

【実施例4】次に、通信販売、インターネットのASP利用の際に、その利用者が所持する携帯可能な情報端末2の電話会社による高信用力の認証を利用することにより、利用料金の課金及び決済する方法とシステムの例について説明する。図17は、通信販売利用したときの流れを示すフローチャートであり、図16は、通信販売利用におけるデータ表例を示す図である。本態様におけるシステムは、基本的に、図1に示されたものに、通信回線15を介して決済管理装置6に接続された携帯可能な又は固定式の利用者端末5を追加したものである。

【0065】まず、利用者は、情報端末5のデータ入力部504から店舗の管理装置1の電話部109に電話接続する(ステップ91)。情報端末5のデータ入力部504を用いて商品データ部108に記録されていた商品の選択し、料金計算・課金部101で料金を計算、課金処理し、これらを通販管理番号とともに記録部106に記録する(ステップ92)。利用者は、さらに、利用者の認証データのうち少なくとも情報端末2の電話番号と自由な暗証番号を入力する。これらデータは、売上時刻とともに記録部506、106に記録される(ステップ93)。

【0066】管理装置1の電話部103は、決済管理装置6に電話をし、サービス・物販識別データと、受信者課金データと、そして、課金データとを送信する(ステップ94)。決済管理装置6は、上記認証データである情報端末2の電話番号と、課金データに、(さらに、サービス・物販識別データ(例えば#0880などの文字列)と、受信者課金データ(例えば#108などの文字列)と、発信者番号通知設定案内と、サービス・物販利

用者識別データ入力案内と、決済データの暗証番号入力案内等を追加しても良い。) 自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置 3 を経由し、情報端末 2 に送信する(ステップ 95)。

【0067】前記()内の追加データの場合も、電話管理装置 3 でサービス・物販識別データと、受信者課金データを認証し、課金データと、決済の諾否問合せデータを情報端末 2 に送信する。電話管理装置 3 では、サービス・物販識別データと、受信者課金データを認証し、課金データと決済の諾否問合せデータを携帯可能な情報端末 2 に送信する(ステップ 96)。利用者は、情報端末 2 で、認証データである情報端末 2 の電話番号と課金データを確認する。(さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。) 自由な暗証番号と決済諾否データである“決済する：1”を入力し、電話管理装置 3 を経由し、決済管理装置 6 に返送する(ステップ 97)。

【0068】決済管理装置 6 は、上記認証データを照合・認証し、記録する(ステップ 98)。合格すると、認証データである情報端末 2 の電話番号と、課金データと、(さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。) 決済許諾データである“決済する：1”を電話管理装置 3 と管理装置 1 に送信する(ステップ 99)。決済管理装置 6 から認証データのうち少なくとも自由な暗証番号と決済の許諾データである“決済する：1”が管理装置 1 に返信されると、管理装置 1 の認証部 105 で認証データのうち少なくとも自由な暗証番号と決済の許諾データである“決済する：1”を認証し、記録部 106 に記録し、売上処理を終了する(ステップ 100)。また、決済の拒否データである“決済しない：0”の返信の場合は、売上処理をせず、キャンセルする。また、決済の方法や高いセキュリティの設定は、ゲート式駐車場利用の例による。

【0069】

【発明の効果】請求項 1 に記載の本発明は、商品・サービスの提供サイトに設けられた管理装置に少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証手順とを含んで構

成されてなるため、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証を各種の非現金決済において必要となる本人であることの認証に利用した本人確認方法を提供することができる効果を有する。

【0070】請求項 2 に記載の本発明は、本人確認を取る手順において、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数とを組み合わせるため、簡単な手順の付加で認証の精度を飛躍的に向上させることができる本人確認方法を提供することができる効果を有する。

【0071】請求項 3 に記載の本発明は、利用者から管理装置への通知手順において、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力するため、適宜の手法で携帯可能な情報端末の電話番号を管理装置に通知することができる本人確認方法を提供することができる効果を有する。請求項 4 に記載の本発明は、本人確認を取る手順において、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を、決済管理装置で照合・認証することから簡単な構成により認証の精度を向上させることができる本人確認方法を提供することができる効果を有する。

【0072】請求項 5 に記載の本発明は、本人確認を取る手順において、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を、決済管理装置で照合・認証することから簡単な構成により認証の精度を向上させることができる他の本人確認方法を提供することができる効果を有する。通常行われている駐車場、店舗の管理装置への電話番号や課金データは、複数の数字や文字を順番に入力し、一遍には入力できない事項である。本発明では、利用者が入力する携帯電話番号は本人が良く知っている事項であり、決済の諾否データも「1」または「0」を入力するだけで足りる利点を有している。また、利用者が入力する電話番号のほか自由な暗証番号、電話登録暗証番号、氏名、郵便番号、年令、住所の一部、電子メールアドレス、支払先金融機関名、口座番号などは本人が良く知っている事項である。従って、本発明では、データ入力が容易で、正確に且つ迅速に処理することができる。

【0073】電話機能を利用することで電話会社の信用力の有る認証機能を利用することができる。また、電話番号を認証データとし電話利用機器の認証と利用者が特

定できる利点を有する。また、電話利用機器と関係する電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号などの認証データで本人を特定し、また、利用するその場で自由な暗証番号を入力することで本人しか分からない一回限りのID番号の認証データを設定することが可能となる利点を有する。従って、これらの認証データを利用者本人が入力し、利用側と支払側の機器を認証することで高度な安全性が保てる。

【0074】また、管理装置1と情報端末2との通信および情報端末2の無線通信により非接触で認証データを入力することで管理装置1、情報端末5などの設置場所から入力していることの特典ができ一層の安全性が保てる。さらにまた、情報端末2で指紋などの生体データを入力し、認証することでも一層の安全性が保てることになる。また、営業などのビジネスにおけるPCやPDAなどの携帯端末からのデータサーバへのアクセスの認証に、現在、持っている携帯電話などを利用して認証でき、容易にシステムを構築できる利点を有している。

【図面の簡単な説明】

【図1】駐車場における本人確認システム及びそれを利用した利用料金決済システムのブロック図である。

【図2】図1に示された管理装置1の詳細構成図である。

【図3】駐車場における管理装置1のデータ入力部104の一例を示す詳細構成図である。

【図4】情報端末2の詳細構成図である。

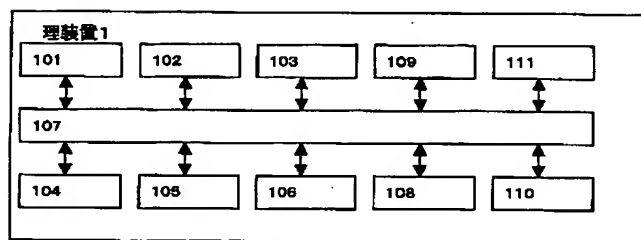
【図5】電話管理装置3の詳細構成図である。

【図6】決済管理装置6の詳細構成図である。

【図7】小売店等の店舗に管理装置1が設置される場合におけるデータ入力部104の詳細構成図である。

【図8】情報端末5の詳細構成図である。

【図2】



【図9】ゲート式駐車場に車を入場する時の流れを示すフローチャートである。

【図10】ゲート式駐車場から車を出庫する時の流れを示すフローチャートである。

【図11】ゲート式及びコイン式駐車場を利用した場合のデータ表の一例である。

【図12】決済管理装置6における決済の流れを示すフローチャートである。

【図13】フラップ式駐車場に入場するときの流れを示すフローチャートである。

【図14】フラップ式駐車場から出場するときの流れを示すフローチャートである。

【図15】店舗で買い物利用したときの流れを示すフローチャートである。

【図16】店舗での買い物利用のデータ表例を示す図である。

【図17】通信販売利用したときの流れを示すフローチャートである。

【図18】通信販売利用におけるデータ表例を示す図である。

【図19】本発明に係る本人確認システムの一実施形態のブロック図である。

【図20】図19に示された本人確認システムによって実行される本発明に係る本人確認方法の一実施形態のフローチャートである。

1 管理装置

2 情報端末

3 電話管理装置

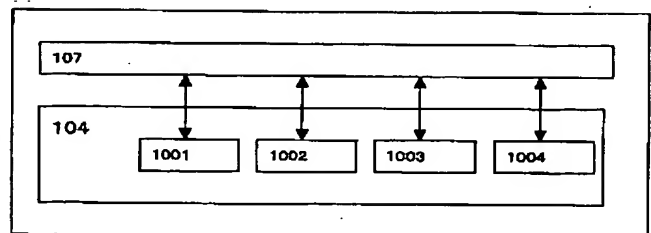
4 決済装置

5 情報端末

6 決済管理装置

12~17 通信回線

【図3】



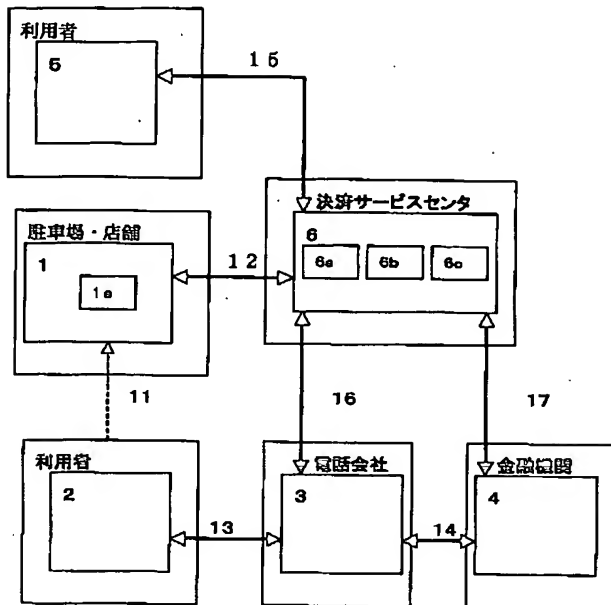
【図11】

* 1	駐車場名	ゲート通過番号	入場時刻	出場時刻	2377番号	入場有無	電話番号	* 2	利用料金(円)
#0880	AABB	入 01/出 02/ 出 03	10:10 2000.07.01	12:15 2000.07.01	—	1	08012347758	#108	900

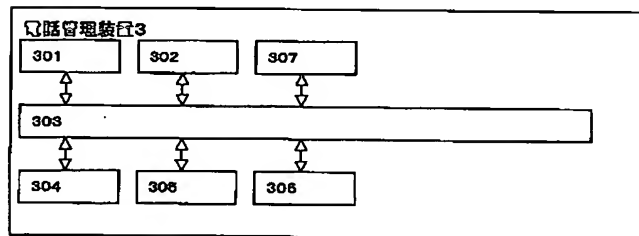
* 1 : サービス・販別データ

* 2 : 受信者課金データ

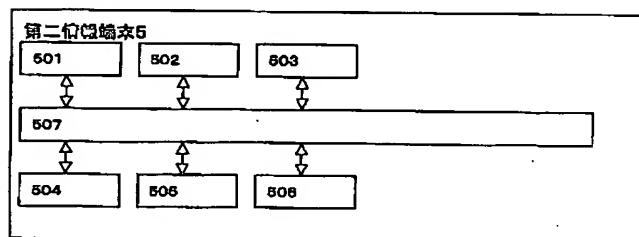
【図1】



【図5】



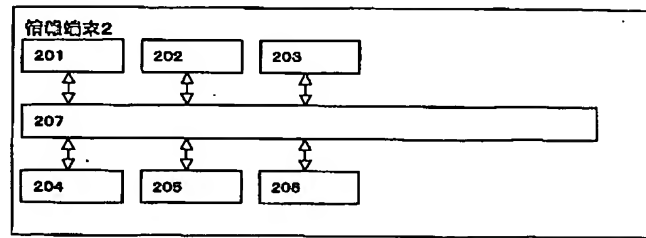
【図8】



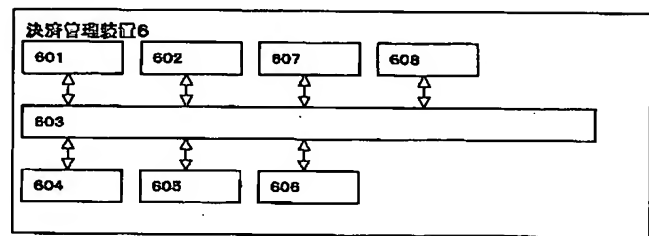
【図16】

年月日	売上時間	口座番号	口座データ	店名	デビットカード番号	口座番号	口座名	店名	売上額(円)
2000.07.01	11:20	08012347788	452	AAAA	007878	A1357	BBBB	2	10,000

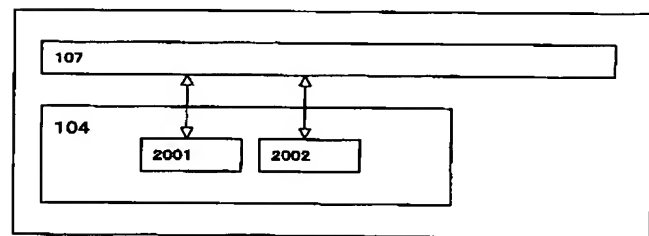
【図4】



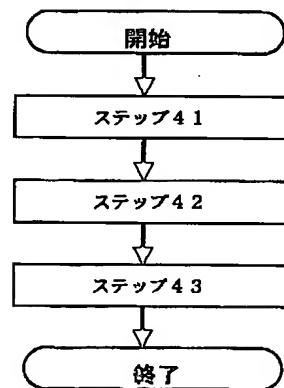
【図6】



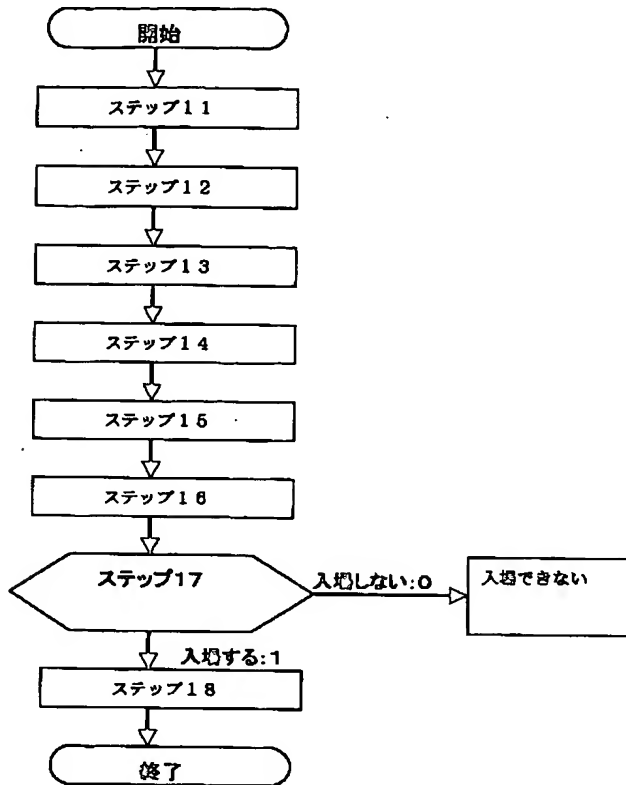
【図7】



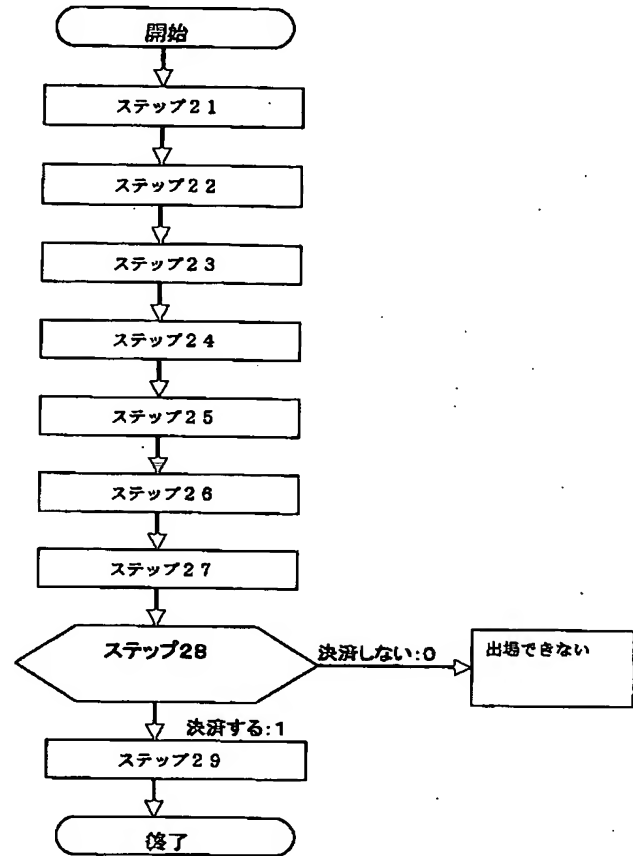
【図13】



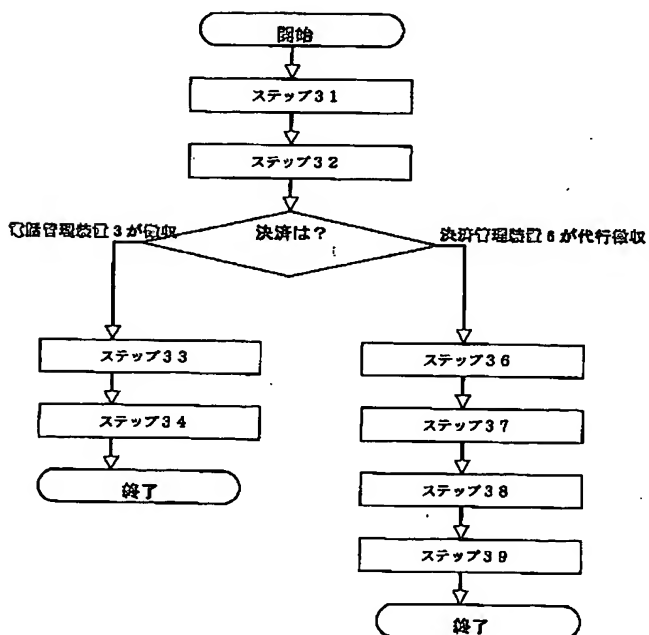
【図 9】



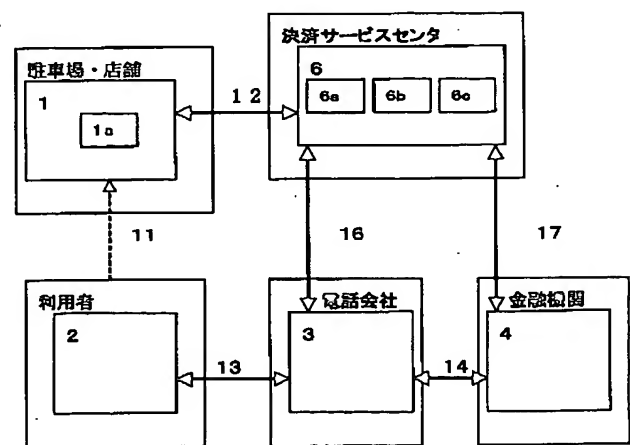
【図 10】



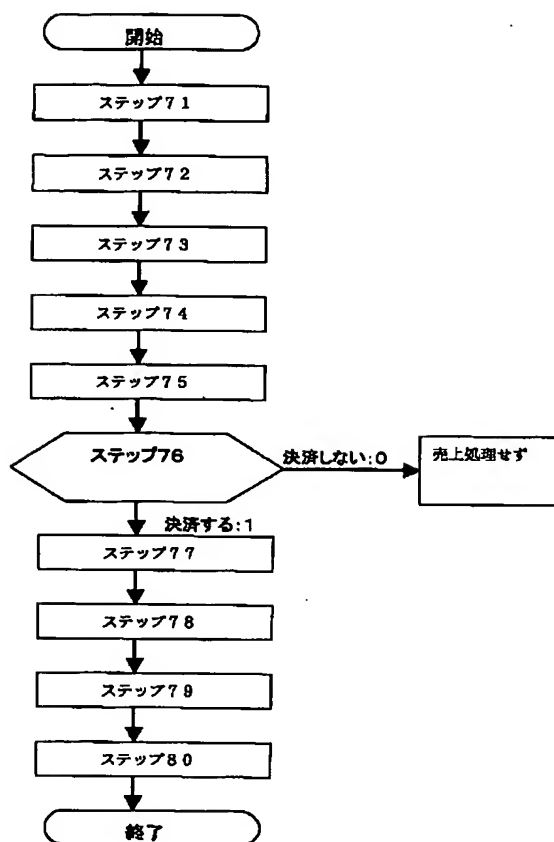
【図 12】



【図 19】



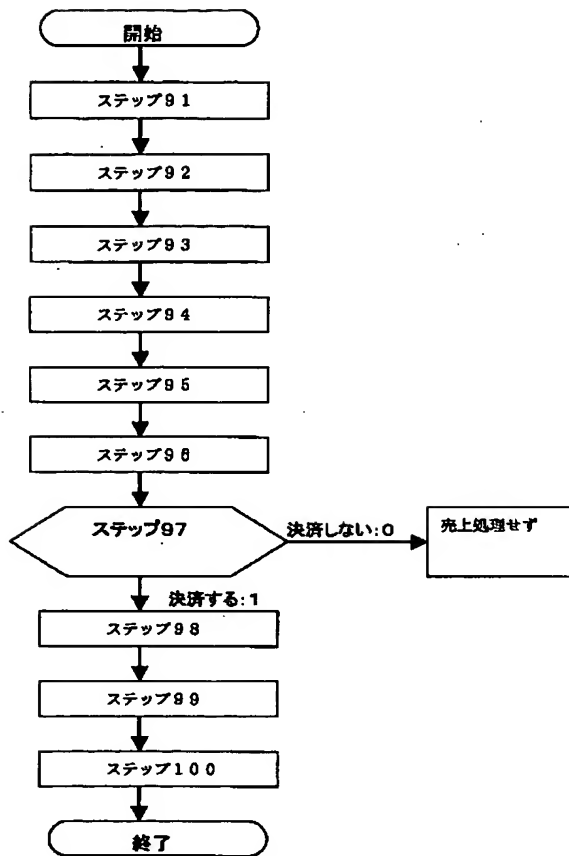
【图 15】



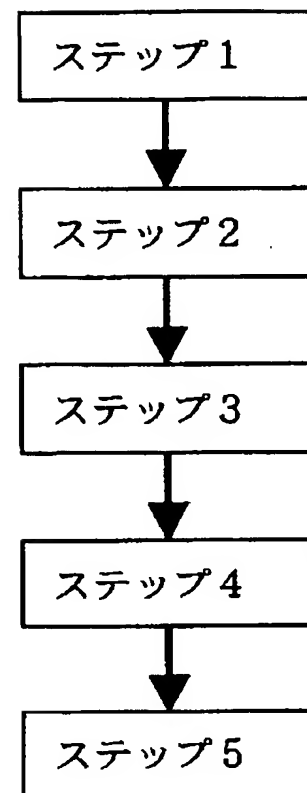
【图 18】

年月日	売上時刻	電話番号	保証データ	通販店鋪名	通販管理番号	商品番号	商品名	数量	売上料金(円)
2000.07.01	11:30	06012347788	452	AAAA	010010	A1857	BBB	3	8,000

【図 17】



【図 20】



フロントページの続き

(72) 発明者 荻田 健之
愛知県名古屋市中区名東区亀の井 1-133 住友
高針荘 A 棟 104 号

(72) 発明者 磯部 俊哉
東京都渋谷区道玄坂 1-21-2 日本航空電
子工業株式会社内

(72) 発明者 森 房夫
東京都渋谷区道玄坂 1-21-2 日本航空電
子工業株式会社内

(72) 発明者 石川 貢司
東京都渋谷区道玄坂 1-21-2 日本航空電
子工業株式会社内

(72) 発明者 大嶋 翼
東京都渋谷区宇田川町 2-1 渋谷ホームズ
1205 号株式会社駐車場総合研究所内

(72) 発明者 小島 雅夫
東京都あきる野市雨間 563-1

F ターム(参考) 5B049 BB11 CC05 CC36 CC46 EE00
GG00 GG06